

Catholic University Law Review

Volume 22
Issue 3 *Spring 1973*

Article 4

1973

Computer Data Bank - Privacy Controversy Revisited: An Analysis and an Administrative Proposal

Grant Morris

Follow this and additional works at: <https://scholarship.law.edu/lawreview>

Recommended Citation

Grant Morris, *Computer Data Bank - Privacy Controversy Revisited: An Analysis and an Administrative Proposal*, 22 Cath. U. L. Rev. 628 (1973).

Available at: <https://scholarship.law.edu/lawreview/vol22/iss3/4>

This Comments is brought to you for free and open access by CUA Law Scholarship Repository. It has been accepted for inclusion in Catholic University Law Review by an authorized editor of CUA Law Scholarship Repository. For more information, please contact edinger@law.edu.

COMMENTS

The Computer Data Bank-Privacy Controversy Revisited: An Analysis and an Administrative Proposal*

Introduction

Despite governmental hearings extending over a period of six years,¹ there is currently no adequate legal protection for the collection and dissemination of information stored in data banks and the future prospect of comprehensive safeguards or even the formulation of policy guidelines appears dim.² Whatever the reasons for Congressional hesitancy into this area, the delay seems unpardonable because governmental intrusions into the private affairs of its citizens through an indiscriminate and unstructured system of collecting information are a present fact which demands the issuance of legislative safeguards.³ In light of the increasing information demand by the

* The author is indebted to Senator Sam Ervin (D.N.C.) and the Subcommittee on Constitutional Rights of the Senate Committee on the Judiciary for supplying information in the preparation of this article.

1. See generally *Hearings on Federal Data Banks, Computers and the Bill of Rights Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary*, 92d Cong., 1st Sess. (1971) [hereinafter cited as *Hearings on Federal Data Banks*]; *Hearings on the Computer and Invasion of Privacy Before the Subcomm. of the House Comm. on Gov't Operations*, 89th Cong., 2d Sess. (1966); *Hearings on Computer Privacy Before the Subcomm. of Administrative Practice and Procedure of the Senate Comm. on the Judiciary*, 90th Cong., 2d Sess. (1968); *Hearings on the Computer and Invasion of Privacy Before the Subcomm. of the House Comm. on Gov't Operations*, 89th Cong., 2d Sess. (1966).

2. This forecast is primarily based on recent Congressional legislation in this area which is very narrow in scope. See, e.g., S. 782, 91st Cong., 1st Sess. (1969); H. Rep. 20, 91st Cong., 1st Sess. (1969); H. Rep. 889, 91st Cong., 1st Sess. (1969); H. Rep. 7214, 91st Cong., 1st Sess. (1969).

3. The computer can already furnish an extensive dossier on nearly every American citizen from the current governmental records which include: fingerprints, police files, military records, court reports, driving records, school records, property holding records, marriage records, employment records, health data, tax returns, security files, credit records, census responses, FHA mortgage guarantees, VA mortgage guarantees, and social security data.

government⁴ and private sectors and the tremendous growth of computer data banks, the future may begin to reflect the pattern of living described in "1984."⁵

Privacy questions that involve stored information⁶ are not solely the result of the development of the computer.⁷ The computer has, however, contributed to the immediacy of the privacy problem and presented another instance of technology advancing without an accompanying legal framework.⁸ The threat to privacy posed by data banks concerns the interest of the individual to live free from unnecessary intrusions or exposures to the outside world.⁹ What is at issue is essentially a balancing process between an individual's interest in nondisclosure and the quest of both the public and private sector for all types of information.¹⁰ Ultimately, the resolution of the problem requires an evaluation of a number of conflicting considerations. The implications of this balancing process are enormous, for at stake is the

4. "The rapid expansion of our Nation's population, its vastly more complicated laws, and the increasing reliance upon statistics to create and evaluate social action programs, have developed an understandable desire to take advantage of advances in computer technology to make Government recordkeeping and analysis more efficient and economical." *House Comm. on Government Operations, Privacy and the National Data Bank Concept*, H.R. Rep., No. 1842, 90th Cong., 2d Sess. (1968) at 1.

5. The specter of the "Big Brother" society was prophesized by GEORGE ORWELL in 1984 (1949); See also A. HUXLEY, *BRAVE NEW WORLD* (1958).

6. A few of the recent popular exposés include: Franklin, *Federal Computers Amass Files on Suspect Citizens*, N.Y. Times, June 28, 1970, at 42, col. 3; Wicker, *In the Nation: A Right Not to be Data-Banked?*, N.Y. Times, July 7, 1970, at 38, col. 3; *Privacy and the Computer*, Wash. Evening Star, Mar. 16, 1970; *In the Name of Security*, Wash. Post, Apr. 24, 1970, at 22, col. 2; Bettelheim, *The Right to Privacy is a Myth*, Saturday Evening Post, July 27, 1968 at 8; Star, *The Computer Data Bank: Will it Kill Your Freedom?* Look, June 25, 1968, at 27; Transcript, *Assault on Privacy*, ABC television broadcast (Sat., Jan. 8, 1972); Transcript, *Under Surveillance*, CBS television broadcast (Thurs., Dec. 23, 1971).

7. For a discussion of the computer-privacy dilemma, see generally Ervin, *The First Amendment: A Living Thought in the Computer Age*, 4 COLUM. L. REV. 13 (1972); Countryman, *The Diminishing Right of Privacy: The Personal Dossier and the Computer*, 49 TEXAS L. REV. 837 (1971); Note, *The Computerization of Government Files: What Impact on the Individual?* 15 U.C.L.A. L. REV. 1374 (1968) (foreword by Mr. Justice Douglas) [hereinafter cited as *The Computerization of Government Files*]; Symposium: *Computers, Data Banks, and Individual Privacy*, 53 MINN. L. REV. 211 (1967); Michael, *Speculations on the Relation of the Computer to Individual Freedom and the Right to Privacy*, 33 GEO. WASH. L. REV. 270 (1964).

8. This paper is not designed to present a thorough review of the right of privacy. For a more complete study of the theory of privacy, see A. BRECKENRIDGE, *THE RIGHT TO PRIVACY* (1970); M. ERNST & A. SCHWARTZ, *PRIVACY: THE RIGHT TO BE LET ALONE* (1962); H. GROSS, *PRIVACY—ITS LEGAL PROTECTION* (1964). See text accompanying notes 12-64, *infra*.

9. For a discussion of the impact of private data collection upon personal privacy, see M. BRENTON, *THE PRIVACY INVADERS* (1964); V. PACKARD, *THE NAKED SOCIETY* (1964).

10. See generally, A. WESTIN, *PRIVACY AND FREEDOM* (1967) [hereinafter cited as *PRIVACY AND FREEDOM*]; A. MILLER, *THE ASSAULT ON PRIVACY* (1971) [hereinafter cited as *ASSAULT ON PRIVACY*].

basic relationship between a private citizen and government.¹¹

Apart from dealing with the *need* to strike a balance between the efficiency of computer operations and the privacy rights of citizens, no attempts have been made to consider what type of controls should be imposed. Nor have standards governing the treatment of computerized information been developed. The questions presented by the conflict between computer data banks and privacy are easily identifiable: What constitutes an invasion of privacy? What is the impact on the individual? What legal protections for computer and data communications presently exist? How should this field be effectively regulated? This comment will consider the desirability of affording adequate and practical legal protection in this area. The consideration is twofold: beginning with an analysis of the proliferation of data banks and the relevant privacy law as it now exists, the author will then propose legislative or administrative safeguards which might be established to insure proper protection.

Privacy—Common Law, State Statutory, and Constitutional Development

Privacy is a vague and elusive concept, and although it has been the subject of much attention, it is still poorly understood.¹² It is considered to be a highly valued right of civilized men and has been characterized by Justice Brandeis as the "right to be let alone."¹³ Although commonly viewed

11. Mr. Justice Douglas has expressed a fear of losing the right to privacy when he stated in *Osborn v. United States*, 385 U.S. 323 (1966) (dissenting opinion):

We are rapidly entering the age of no privacy, where everyone is open to surveillance at all times; where there are no secrets from government. The aggressive breaches of privacy by the Government increase by geometric proportions . . . the dossiers on all citizens mount in number and increase in size. Now they are being put on computers so that by pressing one button all the miserable, the sick, the suspect, the unpopular, the offbeat people of the Nation can be instantly identified. These examples and many others demonstrate an alarming trend whereby the privacy and dignity of our citizens is being whittled away by sometimes imperceptible steps. Taken individually, each step may be of little consequence. But when viewed as a whole, there begins to emerge a society quite unlike any we have seen—a society in which government may intrude into the secret regions of a man's life at will.

Id. at 341-343; see also Mr. Justice Douglas, *Foreword to The Computerization of Government Files* 1374.

12. The volume of literature on privacy is enormous. For an extensive bibliography, see *PRIVACY AND FREEDOM* 445-454.

13. In his treatise on torts, Judge Cooley recognized the right "to be let alone." COOLEY, *TORTS* 29 (2d ed. 1888). The Supreme Court acknowledged Cooley's contribution in *Adair v. U.S.*, 208 U.S. 161, 173 (1908).

It is a part of every man's civil rights that he be left at liberty to refuse business relations with any person, whomsoever, whether the refusal rests upon reason, or is the result of whim, caprice, prejudice or malice. With his reasons neither the public nor third persons have any legal concern.

as a person's interest in secrecy and physical seclusion,¹⁴ privacy need not be restricted to this limited interpretation; rather, some commentators have viewed privacy as a "very special kind of independence," an aspect of human dignity, and a "spiritual interest."¹⁵ Regardless of the interpretation, the term privacy is intimately bound to an individual's interest in nondisclosure of personal information¹⁶ and the ability to control the access of information about oneself.

The protection of privacy in the common law developed in the law of torts.¹⁷ Accordingly, the invasion of a person's privacy is said to constitute a wrong perpetrated by the invader and gives the victim a chance to sue for compensation. The basic foundation for the common law protection was established in 1890 in an article written by Warren and Brandeis calling for recognition of the invasion of privacy as a separate tort.¹⁸ Since that time the right of privacy has been developed to the extent that one authority has subdivided the tort invasion of privacy into four separate doctrines:¹⁹ (1) intrusion upon the seclusion of another; (2) appropriation of another person's name or likeness; (3) publicity that places a person in a false light before the public; and (4) publicity given to another's personal life.²⁰ The common law protection, however, is an inadequate solution to the privacy problem. Despite judicial expansions of the four areas noted above, a significant minority of states still do not recognize a common law right of privacy.²¹

In addition, there are the problems which thwart attempts to protect one individual's privacy against encroachment by the computer. These include the following: the lack of a precise definition of privacy which would encompass the scope and nature of the right protected; the inadequate classifications of privacy suits as defamation actions and the subsequent lack of relief afforded to the disclosure of personal information in the absence of malice; the deterrence factors of time, exposure, and emotion as-

14. W. PROSSER, *THE LAW OF TORTS* 33 (3d ed. 1964); 1 F. HARPER & F. JAMES, *THE LAW OF TORTS* § 9.6 at 682 (1956).

15. For an excellent discussion of the concept of privacy as a necessary context for love, friendship and trust, see Fried, *Privacy*, 77 *YALE L.J.* 475 (1968).

16. See generally the section on privacy in 31 *LAW AND CONTEMPORARY PROBLEMS* 251 (1966).

17. See the court's explanation in *Pavesich v. New England Life Insurance Co.*, 122 Ga. 190, 50 S.E. 68 (1905).

18. Warren and Brandeis, *The Right to Privacy*, 4 *HARV. L. REV.* 193 (1890).

19. Prosser, *Privacy*, 48 *CALIF. L. REV.* 383, 383-386 (1960). See *RESTATEMENT (SECOND) OF TORTS* § 652A (Tent Draft No. 13, 1967).

20. The approach by Professor Prosser to the right of privacy has been criticized. See Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 *N.Y.U.L. REV.* 962 (1964).

21. W. PROSSER, *THE LAW OF TORTS* § 112, at 831 (3d ed. 1964).

sociated in having to go to court to settle a claim; the erroneous presumption that the individual is aware of the violation which is said to be nearly impossible to detect; the difficulty in overcoming such barriers as the doctrine of sovereign immunity in an action against the government; and the fact that the common law affords essentially a remedial and compensatory protection rather than providing strict preventive measures.²²

State statutes designed to protect privacy have been enacted in 39 jurisdictions.²³ These laws may be seen as primarily a response to the failure of the common law to provide a right of privacy and to give further protection to other statutory provisions which apply to official records.²⁴ In 1903 New York became the first state to recognize an intrusion into the "right to be let alone." Following a highly controversial decision by the New York Court of Appeals²⁵ that was supplemented by one of the judges writing a law review article,²⁶ the New York legislature enacted a statute which made it both a misdemeanor and a tort to publish, without permission, the names or likenesses of living persons for commercial purposes.²⁷ Later in 1934, the Restatement of Torts approved a cause of action for "unreasonable and serious" interferences with privacy.²⁸ These developments prompted greater recognition of privacy rights by the courts and the state legislatures.

As was true of the very incomplete protection of the right of privacy afforded by the common law, state statutes are similarly inadequate. Even though nearly all states have legislative provisions dealing with the accessibility of official records,²⁹ state restrictions on the availability of such records has been criticized as being unclear and oftentimes left to the discretion of the keeper of the records.³⁰ Moreover, the privacy protection under the more recent legislation which prohibits eavesdropping and electronic surveillance of conversations is not applicable to computer communications. Hence, state statutory provisions are largely ineffective as a remedy for these privacy intrusions.

22. See generally Miller, *Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society*, 67 MICH. L. REV. 1091 (1969).

23. This section on state statutes and their privacy related provisions relies heavily on Prosser, *supra* note 21, at 829-51.

24. Meldman, *Centralized Information Systems and the Legal Right to Privacy*, 52 MARQ. L.R. 342 (1969).

25. *Roberson v. Rochester Folding Box Co.*, 171 N.Y. 538, 64 N.E. 442 (1902). This decision repudiated lower court decisions which had accepted the right of privacy.

26. O'Brien, *The Right of Privacy*, 2 COL. L. REV. 437 (1902).

27. N.Y. Sess. Laws, ch. 132 § 1-2 (1903). Amended in N.Y. Civil Rights Law, § 50-51 (1921).

28. RESTATEMENT OF TORTS, AMERICAN LAW INSTITUTE, 67 (1934).

29. Meldman, *supra* note 24 at 343.

30. Karst, *The Files: Legal Controls Over the Accuracy and Accessibility of Stored Personal Data*, 31 LAW & CONTEMP. PROB. 342, 348 (1968).

The Constitution is devoid of any mention of a "right to privacy"³¹ and, as a result, privacy has developed to a large extent in connection with certain amendments to the Constitution prohibiting various intrusions by the government.³² Acquisition of information may constitute a violation of: the first amendment's protection of free speech and privacy in one's association, the fourth amendment's protection against unreasonable search and seizures, the fifth amendment's guarantee against self-incrimination, and the fourteenth amendment's due process protection.³³

A first amendment right of associated privacy was established by the Supreme Court in *NAACP v. Alabama*³⁴ as the freedom to associate and privacy in one's association.³⁵ Two years afterwards the Court in *Talley v. California*³⁶ extended the *NAACP* ruling by emphasizing the necessity of anonymous political activity in striking a California ordinance requiring the names of the author and distributor to be printed on handbills.³⁷ Later, in *Gibson v. Florida Investigating Committee*³⁸ the rights of association were held to be within the ambit of the constitutional protections afforded by the first and fourteenth amendments. "And it is equally clear that the guarantee encompasses protection of privacy of organizations NAACP such as that of which the petition is president."³⁹

The relation of the first amendment rights of free speech and associated privacy to the privacy problem in computerized information is manifest in

31. However, many courts are willing to recognize a right of privacy. For example, see *Afro-American Publishing Co. v. Jaffe*, 366 F.2d 649 (D.C. Cir. 1966). . . . the right of privacy stands on high ground, cognate to the values and concerns protected by constitutional guarantees . . . [and] . . . is crucial to the vitality of democracy. *Id.* at 654.

32. Although there may be no specific "right to privacy," according to one commentator:

. . . it is hard to see how several of the specific rights in the Constitution can be given a meaningful scope without necessarily safeguarding a right to privacy. It would be indeed ironic if this were not so in a constitutional system designed to protect the integrity of the individual in an age that laid stress on the necessity of recognizing both the rational and irrational elements in man but which, above all, wanted to protect his dignity and status as an individual.

Beane, *The Right to Privacy and American Law*, 31 LAW AND CONTEMP. PROB. 253, 260 (1966); see also Beane, *The Constitutional Right to Privacy in the Supreme Court*, 1962 SUP. CT. REV. 212.

33. The Ninth Amendment may also be included. See the interpretation by Mr. Justice Goldberg in *Griswold v. Connecticut*, 381 U.S. 479, 488-94 (1965) (concurring opinion). See also text accompanying notes 49-52 *infra*.

34. 357 U.S. 449 (1958).

35. *Id.* at 466.

36. 358 U.S. 60 (1960).

37. *Id.* at 64.

38. 372 U.S. 539 (1963).

39. *Id.* at 544.

the case of *Anderson v. Sills*.⁴⁰ The controversy concerned the Sills Memorandum⁴¹ which set forth a plan to cope with possible civil disorders in New Jersey.⁴² The plan directed local law enforcement officials to file reports for any civil disturbance, rally, protest, demonstration, march, or confrontation.⁴³ Also included was a proposal to list the names of "leaders" and "organizations and/or groups" involved.⁴⁴ In ruling that the information gathering plan of the Sills Memorandum was too broad, the trial court concluded that: "[I]t is not too difficult to imagine the reluctance of an individual to participate in any kind of protected conduct which seeks publicly to express a particular or unpopular political or social view because . . . by doing so he might now have a record, or because his wife, his family or his employer might also be included in the data book. . . ." ⁴⁵

The fourth amendment's prohibition against unreasonable searches and seizures has been summarized by Mr. Justice Frankfurter as: "The security of one's privacy against arbitrary intrusion by the police—which is at the core of the Fourth Amendment—is basic to a free society."⁴⁶ The characterization of the fourth amendment as the "right to be let alone" has received support by Mr. Justice Brandeis when he observed that it is "the most comprehensive of rights and the right most valued by civilized men,"⁴⁷ and by Mr. Justice Douglas when he expressed that "the right to be let alone is indeed the beginning of all freedom."⁴⁸

In *Griswold v. Connecticut*,⁴⁹ the Supreme Court presented the clearest articulation to date of privacy as an independent right.⁵⁰ Declaring the ex-

40. 106 N.J. Super. 546, 256 A.2d 298 (Ch. 1969).

41. The memorandum was officially entitled, *Civil Disorders—The Role of Local County and State Government*.

42. For a comprehensive evaluation of the Sills Memorandum and the "chilling effect" of data gathering programs, see Askin, *Police Dossiers and Emerging Principles of First Amendment Adjudication*, 22 STAN. L. REV. 196 (1970).

43. Sills Memorandum, Instructions for Preparing the Security Incident Report, Instruction 9, 106 N.J. Super. at 559, 256 A.2d at 306 (1969).

44. *Id.* at 560, 256 A.2d at 307.

45. *Anderson v. Sills*, 106 N.J. Super. at 556, 256 A.2d at 304. On appeal, the New Jersey Supreme Court reversed the Superior Court's decision but did indicate that if, on an evidentiary hearing it could be shown that a chilling effect on the freedom of expression had occurred, then the court would proceed to look into the matter.

46. *Wolf v. Colorado*, 338 U.S. 25, 27 (1949).

47. *Olmstead v. United States*, 277 U.S. 438, 478 (1928); *Cf. Berger v. New York*, 388 U.S. 41 (1967).

48. *Public Util. Comm'n v. Pollak*, 343 U.S. 451, 467 (1952) (Douglas J., dissenting); Mr. Chief Justice Burger has recently commented on this valuable right when he said ". . . the right of every person 'to be let alone' must be placed in the scales with the right of others to communicate." *Rowan v. Post Office Dep't*, 397 U.S. 728, 736 (1970).

49. 381 U.S. 479 (1965).

50. See generally Dixon, *The Griswold Penumra: Constitutional Charter For An Expanded Law of Privacy?*, 65 MICH. L. REV. 197 (1965).

istence of certain "zones of privacy" to be protected under the "penumbra" of the first, third, fourth, fifth, and ninth amendments,⁵¹ the Court held that a Connecticut contraceptive law violated the right of privacy of married persons. Although two Justices disagreed,⁵² the majority in *Griswold* considered the right to privacy as a separate constitutional doctrine. This rationale has been recently extended in *Nader v. General Motors Corp.* to include invasions of privacy by a public corporation.⁵³

The privacy protection under the fourth amendment is complemented by the fifth amendment's privilege against self-incrimination.⁵⁴ In *Boyd v. U.S.*,⁵⁵ the Supreme Court pointed to the "intimate relation" between the two amendments when it invalidated a law requiring the defendant to produce documents or have the government's charges admitted.⁵⁶ Faced with a fifth amendment plea by a witness before a Congressional investigating committee, the Court in *Watkins v. U.S.*⁵⁷ gave recognition to the potentially harmful exposure of the private affairs of individuals.⁵⁸ Furthermore, in *Tehan v. Shott*,⁵⁹ the Court declared that the fifth amendment is basically an ex-

51. Referring to the first, third, fourth and fifth amendments, the majority held that, "specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance . . . [which] create zones of privacy." *Griswold v. Connecticut*, 381 U.S. 479, 484 (1965).

52. Mr. Justice Black and Mr. Justice Stewart both wrote separate dissenting opinions, each denying the existence of a right of marital privacy protected by the Constitution. Mr. Justice Black criticized the majority for emphasizing a right of privacy. He complained:

One of the most effective ways of diluting or expanding a constitutionally guaranteed right is to substitute for the crucial word or words of a constitutional guarantee another word or words, more or less flexible and more or less restricted in its meaning. This fact is well illustrated by the use of term 'right of privacy'. As a comprehensive substitute for the Fourth Amendment's guarantee against unreasonable searches and seizures' . . . I get nowhere in this case by talk about a constitution 'right of privacy' as an emanation from one or more constitutional provisions.

Id. at 509-10.

53. Misc. 2d 301, 292 NYS 2d 514 (Sup. Ct. 1968), *aff'd* 298 NYS 2d 137 (App. Div. 1969), *cf.* *United States v. Rictenbucker*, 209 F.2d 462 (2nd Cir. 1962); *Katz v. United States*, 389 U.S. 147 (1967).

54. It has been suggested that the fifth amendment's prohibition of the taking of private property by the government should likewise be extended to include an intrusion of the right of privacy. Comment, *Privacy, Property, Public Use, and Just Compensation*, 41 S. CAL. L. REV. 902, 909 (1968).

55. 116 U.S. 616 (1885).

56. *Id.* at 633.

57. 354 U.S. 178.

58. *Id.* at 200. Nevertheless, the *Watkins* decision was severely limited by the Supreme Court in *Barenblatt v. U.S.*, 354 U.S. 178 (1969). Writing for the majority, Mr. Justice Harlan said:

We conclude that the balance between the individual and the governmental interests here at stake must be stuck in favor of the latter, and that therefore the provisions of the First Amendment have not been offended. *Id.* at 134.

59. 382 U.S. 406 (1966).

tension of the right to privacy and the "respect for the inviolability of the human personality and of the right of each individual 'to a private enclave where he may lead a private life'." ⁶⁰

In addition, if the acquisition of unfavorable information about a person is accomplished without providing notification to the individual, the due process clause of the fourteenth amendment may well be violated. In *Constantineau v. Wisconsin*,⁶¹ the Supreme Court invalidated a Wisconsin statute permitting a police chief to post a list of persons in the town who he believed to be alcoholics. Speaking for the Court, Mr. Justice Douglas said, "Where a person's good name, reputation, honor, or integrity are at stake because of what the government is doing to him, notice and an opportunity to be heard are essential."⁶² The *Constantineau* decision thus indicates that a citizen may have the protection of due process with regard to the circulation of information concerning him.

Despite the attempts of the judicial system in delineating an area of protected privacy, it remains to be seen whether the information-privacy area will be extended constitutional protection. To expect such protection appears unduly optimistic because even in *Griswold* the Court carefully avoided defining privacy and instead chose to play "charades with the Constitution."⁶³ In view of the tremendous growth of the use of computers and the acceleration of accumulated and stored data in America's "record keeping civilization,"⁶⁴ waiting for further constitutional interpretation appears to be far too uncertain and hazardous.

Computer Data Banks as a Threat Posed to the Individual

In what has been characterized as the "Computer Revolution," and the "Age of Cybernetics," we are currently witnessing in this country the phenomenal growth of a machine called the "computer." The computer, in its brief 26 year history, has completely revolutionized the information process by drastically increasing man's capacity to accumulate, manipulate, retrieve, and transmit information. Data banks are the means by which computers are utilized in the process of storing information, and since the computer is capable of holding a vast amount of information a new source of power has thus been created.⁶⁵

To an increasing degree the activities of the government require extensive

60. *Id.* at 414.

61. 400 U.S. 433 (1971).

62. *Id.* at 437.

63. Dixon, *supra* note 50, at 218.

64. Karst, *supra* note 30, at 342.

65. See generally A. WESTIN, INFORMATION TECHNOLOGY (1971).

record keeping facilities and the government has turned to the computer to help solve this problem.⁶⁶ This need for information has been the result of the growing complexity and expansion of governmental operations.⁶⁷ A desire to collect information concerning the operation of society in general in order to understand the social and the economic forces at work and thereby construct sound policies that are designed to change underlying conditions does not create problems that are the subject of this article. When information is accumulated about individuals, however, which begins to resemble "dossier" files, this situation presents a genuine threat to personal privacy. Nevertheless, this latter type of compilation has been the trend in recent years.⁶⁸

Whenever information about someone is gathered, three basic interests of the individual are in jeopardy. First is a person's right to withhold certain information except to those to whom he exclusively consents. Second is the possibility of a factual⁶⁹ or contextual inaccuracy⁷⁰ which could create an erroneous impression. As one commentator explains, "any of this information might be entirely accurate and sufficient when viewed from one perspective but be wholly incomplete and misleading when read in another."⁷¹ Third is the potential "intimidation by information"⁷² which might

66. See Shils, *Privacy and Power*, in *Hearings on Computer Privacy Before the Subcomm. on Administrative Practice and Procedure of the Senate Comm. on the Judiciary*, 90th Cong., 1st Sess. 231 (1967).

67. See Symposium: *Computers, Data Banks, and Individual Privacy*, 53 MINN. L. REV. 211, 215 (1968) (Remarks by Richard Ruggles).

68. See e.g. *ACLU v. Westmoreland*, 70 Av. 3191 (N.D. Ill., Jan. 5, 1971); *Fifth Avenue Peace Parade Committee v. Hoover*, 70 Civ. 2646 (S.D.N.Y. 1971); *Hentoff v. Ichord*, 318 F. Supp. 1175 (D.D.C. 1970); *Menard v. Mitchell*, 430 F.2d 486 (D.C. Cir. 1970); *Tatum v. Laird*, 408 U.S. 1 (1972). In *Laird*, the Supreme Court denied the existence of a justiciable controversy concerning an ACLU-sponsored suit which challenged the Army's domestic intelligence system.

69. This is usually the problem of the half-truth which is "most graphically illustrated by the unexplained and incomplete arrest record. It is unlikely that a citizen whose file contains an entry 'arrested, 6/1/42; convicted felony 1/6/43; three years, federal penitentiary' would be given federal employment or be accorded the governmental courtesies accorded other citizens. Yet the subject may simply have been a conscientious objector. And what about the entry 'arrested, disorderly conduct; sentenced six months Gotham County Jail.' Without further explanation, who would know that the person was a civil rights demonstrator whose conviction was reversed on appeal?" Miller, *The National Data Center and Personal Privacy*, THE ATLANTIC MONTHLY, 53, 55 (Nov. 1967).

70. "The danger of inaccuracy lies in the fact that the evaluator and the recipient of his statement may not share the same standards for reducing a complex set of facts to evaluate inferences or even the same language . . ." Karst, *supra*, note 30, at 359.

71. ASSAULT ON PRIVACY 33.

72. See generally, Comment, *Secret Files: Legitimate Police Activity or Unconstitutional Restraint on Dissent?* 58 GEO. L.J. 569 (1970); Note, *Chilling Political Expression by Use of Police Intelligence Files*, 5 HARV. CIV. RIGHTS—CIV. LIB. L. REV. 71 (1970); Note, *The Chilling Effect in Constitutional Law* 69 COLUM. L. REV. 808 (1969).

result in an inhibiting effect on the exercise of one's constitutional freedoms such as free speech and assembly.⁷³

An individual's concern in nondisclosure of information necessarily involves an aspect of a psychological nature.⁷⁴ Although the potential psychological impact of unregulated information handling is speculative, studies have confirmed that man strives for privacy at various times and in varying degrees.⁷⁵ Inherent in the public's greater awareness that significant amounts of information are being kept on file is the notion that man does not have a meaningful existence apart from his file. The individual is said to believe that he is what the file says.⁷⁶ Essentially this belief is rooted in one's individual identity or conceptualization of oneself.⁷⁷ According to psychologists, self-identification is the process by which the individual evaluates himself as he perceives it through the eyes of others.⁷⁸ Due to the prospects of either unfavorable or highly personal information being exposed to the outside world, man will severely limit his potential for achieving self-actualization.⁷⁹

The unforgetting and unforgiving computer has virtually eliminated the possibility of a "fresh start" in life. Disclosure of personal information has resulted in what is commonly referred to as a "record prison."⁸⁰ Accord-

73. "Inhibition as well as prohibition against the exercise of precious First Amendment rights is a power denied to government." *Lammond v. Postmaster General*, 381 U.S. 301, 309 (1965) (Brennan, J., concurring). One authority has declared "... it cannot be doubted that governmental surveillance and maintenance of detailed dossiers on persons who engage in active protest against government institutions and policies constitute a burden that may deter the more cautious and discreet from engaging in protest activities. The police activity here, no less than the listing scheme in *Lamond*, would appear to be 'at war with the 'uninhibited, robust, and wide open' debate and discussion that are contemplated by the First Amendment.'" Askin, *Police Dossiers and Emerging Principles of First Amendment Adjudication*, 22 STAN. L. REV. 196 (1970).

74. For a discussion on the interests of the individual in nondisclosure of personal information see, *The Computerization of Government Files* 1412-1425.

75. See generally, A. MOSLOW, *MOTIVATION AND PERSONALITY*, 212-13, 227 (1954); E. GOFFMAN, *THE PRESENTATION OF SELF IN EVERYDAY LIFE*, 69-70 (1959); K. LEWIN, *RESOLVING SOCIAL CONFLICTS*, 18-35 (1948); cf. E. HALL, *THE HIDDEN DIMENSION*, 108-112 (1966).

76. ASSAULT ON PRIVACY 49.

77. Michael, *Speculations on the Relation of the Computer to Individual Freedom and the Right to Privacy*, 33 GEO. WASH. L. REV., 270, 278-79 (1964).

78. For example, it has been said that "without privacy there is no individuality. There are only types. Who can know what he thinks and feels if he never has the opportunity to be alone with his thoughts and feelings?" L. YOUNG, *LIFE AMONG THE GIANTS* 26 (1966); see also D. DELEVITA, *THE CONCEPT OF IDENTITY*, 96-120 (1965).

79. *The Computerization of Governmental Files* 1419; This view has been characterized as the mirror-image concept of self-identification. See generally, A. STRAUSS, *MIRRORS AND MASKS* (1959).

80. PRIVACY AND FREEDOM 160; "Computerized central storage of information would remove what surely has been one of the strongest allies of the claim to

ing to this view, stored information can create a situation whereby "past mistakes, omissions, or misunderstood events become permanent evidence capable of controlling destinies for decades. Out-of-date facts, such as previous political affiliations or nervous disorders, often go unrevised, and these can haunt a person's life."⁸¹ Furthermore, another psychological manifestation of centralized dossier-type information systems upon the individual is the potential loss of confidence and distrust towards the government and private organizations using these systems.⁸² As stated by one psychologist, mutual distrust and hostility characterizes the behavior patterns in a society which fails to protect privacy.⁸³

Personal information contained in a computer dossier represents a potential for exposure of private facts. Regardless of whether the facts are improperly disseminated by "unauthorized use" or by the inaccuracy or incompleteness in the information itself, the danger remains. Erroneous, superfluous, hearsay, and outdated information contained in present credit and criminal dossiers clearly illustrate a few of the dangers in information collection and reflect the urgent need for safeguards.⁸⁴

In the past, governmental and private agencies have remained independent in their information gathering and the use of computers has been restricted to each agency seeking to meet its individual needs. Due to the inherent difficulties in such decentralization,⁸⁵ it was not surprising in 1965 to find the Bureau of the Budget proposing that a National Data Bank be established which would collect and standardize the statistics gathered by twenty federal agencies.⁸⁶ Although this proposal has been reviewed by several Congressional committees and there is currently no fully developed plan for a National Data Center,⁸⁷ the implications of overemphasizing efficiency at the expense of privacy rights of citizens remains largely unanswered.

privacy—the inefficiency of man and the fallibility of memory." Ruebhausen and Brim, *Privacy and Behavioral Research*, 65 COLUM. L. REV. 1184, 1189 (1965).

81. PRIVACY AND FREEDOM 160.

82. Cf. ASSAULT ON PRIVACY 52.

83. Katzell, *Psychological Investigation and the Right of Privacy*, 17 VA. LAW WEEKLY, DICTA 109-110 (1964-66).

84. See generally, note 1, *supra*.

85. Duplication of effort and high-costs which result in a largely inefficient operation are the major disadvantages of decentralization. However, decentralization also serves as a barrier to comprehensive dossiers on individuals when there is no intercommunication between computer units.

86. See generally, Note, *Privacy and Efficient Government: Proposals for a National Data Center*, 82 HARV. L. REV. 400 (1968); Zwick, *A National Data Center*, American Bar Association, Section of Individual Rights and Responsibilities, Monograph No. 1, at 32 (1967).

87. See note 159 *infra*.

In the public domain⁸⁸ at present the following federal agencies or departments are compiling files on individuals.⁸⁹ The Federal Bureau of Investigation is connected to at least 24 computerized terminals and contains more than 17 million personal files;⁹⁰ the Internal Revenue Service has a file on everyone who files a federal income tax return;⁹¹ the House Internal Security Committee has a cumulative index for the period 1938-54⁹² and a 1970 supplement which contains a total of 63,000 names;⁹³ the Civil Service Commission has a list of 2,120,000 names in its "security file" and another 10,250,000 files in its "security investigations index;"⁹⁴ the Secret Service has a list of 100,000 names and has produced 50,000 dossiers;⁹⁵ the Department of Defense has a list containing 25 million names;⁹⁶ the United States Army maintains a central index with more than seven million files in its Investigative Records Depository;⁹⁷ and the Justice Department has approximately five million files.⁹⁸ Furthermore, the Department of Housing

88. Since the Census Bureau is interested only in groups and not individuals, it was included from the list of agencies. However, Senator Ervin has said that the Census Bureau makes greater use of computer technology for personal inquiries than any other agency. Ervin, *The First Amendment: A Living Thought in the Computer Age*, COLUM. HUMAN RIGHTS L. REV. 13, 32 (1972). Moreover, it should also be noted that the Census Bureau obtains information from other agencies. See generally, *Hearings on 1970 Census Questions Before the House Comm. on Post Office and Civil Service*, 89th Cong., 2d Sess. 28 (1966); *Hearings on S. 1791 and Privacy, the Census and Federal Questionnaires Before the Subcomm. on Constitutional Rights of the Senate Judiciary Committee*, 91st Cong., 1st Sess. (1969).

89. According to Senator Ervin (D., N.C.), Chairman of the Subcommittee on Constitutional Rights, the "[s]ubcommittee undertook a survey to discover what computerized and mechanized data banks government agencies maintain on people, especially about their personal habits, attitudes, and political behavior. We have also sought to learn what government-wide or nationwide information systems have been created by integrating or sharing the separate data bases. Through our questionnaire, we have sought to learn what laws and regulations govern the creation, access and use of the major data banks in government." Ervin, *The First Amendment: A Living Thought in the Computer Age*, 4 COLUM. HUMAN RIGHTS L. REV. 13, 17 (1972); See also, *Secrecy in a Free Society*, 213 NATION 454 (1971); Ervin, *Privacy and Governmental Investigations*, 1971 U. ILL. L. FORUM 137 (1971).

90. *Hearings on Dep't of Justice Appropriations for 1971 Before a Subcomm. of the House Comm. on Appropriations*, 91st Cong., 2d Sess., 692, 694 (1970).

91. Cf. Clurman and Provorny, *Publicity and Inspection of Federal Tax Returns*, 46 TAXES 144 (1968).

92. Cumulative Index to Publications of the Comm. on Un-American Activities 1938-54, at 15-961 (1962).

93. Supplement to Cumulative Index to Publications of the Comm. on Un-American Activities 1955-68, at 19-587 (1970).

94. Response to the questionnaire by the Subcommittee on Constitutional Rights, in Subcommittee files, March 25, 1971 and on file at the Catholic University Law Review office.

95. Boston Herald-Traveler, April 19, 1970, at 43, col. 1.

96. N.Y. Times, Feb. 13, 1971, at 31, col. 1.

97. Response to the questionnaire by the Subcommittee on Constitutional Rights, in Subcommittee files, Aug. 1970, and on file at the Catholic University Law Review office.

98. *Id.*

and Urban Development has recently suggested an integration of its computer files with those of the Federal Housing Administration, the Justice Department, and the Federal Bureau of Investigations. These records, coupled with other records such as Social Security, police, medical and the like, total an estimated 2.8 billion pieces of information about individuals which could be pooled.⁹⁹

Data banks at the county, state, and regional levels have also proliferated nearly as rapidly as those in the federal government.¹⁰⁰ Perhaps the most significant development is the creation of the New York State Identification and Intelligence System (NYIIS) which provides state and local law enforcement agencies with information about persons with arrest and conviction records, wanted persons, gun registrations, and narcotics addicts.¹⁰¹ Chicago, St. Louis, and many other large cities have developed similar sophisticated computer systems to maintain files on criminal activity in their areas.¹⁰²

In the private domain, information collectors have been establishing their own "integrated information systems," and have expressed a desire to connect these nonfederal data banks to the government information centers.¹⁰³ Currently, there are 2,500 credit bureaus in this country, with the Associated Credit Bureau's Inc. being the largest.¹⁰⁴ This bureau has records on approximately 100 million persons and engages in an interchange of information with other affiliated bureaus.¹⁰⁵

99. Robertson, *Data Bank: Peril or Aid*, N.Y. Times, Jan. 7, 1968, at 1, col. 6. See also, *Hearings on Computer Privacy Before the Subcomm. of Administrative Practice and Procedure of the Senate Comm. on the Judiciary*, 90th Cong., 1st Sess. 19, 26-27 (1967).

100. See, e.g., *A City Where Computers Will Know Everybody*, U.S. NEWS AND WORLD REPORT, April 8, 1968, at 82.

101. See PRESIDENT'S COMMISSION OF LAW ENFORCEMENT AND THE ADMINISTRATION OF JUSTICE, TASK FORCE REPORT: SCIENCE AND TECHNOLOGY 72 (1967).

102. Katzebach and Tome, *Crime Data Centers: The Use of Computers in Crime Detection and Prevention*, 4 COLUM. HUMAN RIGHTS L. REV. 49, 51 (1972).

103. Congressional investigation of commercial agencies has been extensive. See, *Hearings on Commercial Credit Bureaus Before the Special Subcomm. on Invasion of Privacy of the House Comm. on Gov't Operations*, 90th Cong., 2d Sess. (March 1968); *Hearings on Retail Credit Co. of Atlanta Before the Special Subcomm. on Invasion of Privacy of the House Comm. on Gov't Operations*, 90th Cong., 2d Sess. (May 1968); *Hearings on S. Res. 233 Before the Subcomm. on Antitrust and Monopoly of the Senate Judiciary Comm.*, 90th Cong., 2d Sess. (December 1968); *Hearings on S. 823 before the Subcomm. on Financial Institutions of the Senate Banking and Currency Comm.*, 91st Cong., 1st Sess. (May 1969); *Hearings on H.R. 16340 Before the Subcomm. on Consumer Affairs of the House Comm. on Banking and Currency*, 91st Cong., 2d Sess. (March-April 1970).

104. See generally, Comment, *Credit Investigations and the Right to Privacy: Quest for a Remedy*, 57 GEO. L.J. 509 (1969); Comment, *Agency Access to Credit Bureau Files: Federal Invasion of Privacy?* 12 B.C. IND. & COM. L. REV. 110 (1970).

105. Countryman, *The Diminishing Right of Privacy: The Personal Dossier and the Computer*, 49 TEXAS L. REV. 837, 839 (1971).

Similarly, private investigatory agencies which are designed to supplement credit bureaus files have grown considerably. The Atlanta based Retail Credit Company contains 48 million files,¹⁰⁶ the Hooper-Holmes Bureau Inc. contains nine million files,¹⁰⁷ and the TRW Credit Data Company contains 40 million files.¹⁰⁸ The net result of this growth is that the exchange of private information about individuals is likely to occur between thousands of private and governmental data banks.

The threat to privacy rights posed the above noted information gathering cannot be overstated. Although the media has publicized the problems inherent in the information collecting ability of one large centralized data bank,¹⁰⁹ it would seem that this receives an exaggerated amount of attention and concern by the public when compared to what is a more encompassing problem of sophisticated interconnected systems which enable the government to coordinate the information gathering programs of the many agencies. Since each federal agency is said today to constitute its own data center,¹¹⁰ the prospect of federal information inter-communication¹¹¹ is an immediate concern.¹¹² A system of this nature could readily be connected into a massive comprehensive network of federal, state, and local information systems. With the growing trend towards remote-access time sharing systems, the computer and communication technologies appear to be permanently intertwined.¹¹³ While centralization and inter-communication be-

106. *Hearings on S. 823 Before the Subcomm. on Financial Institutions of the Senate Banking and Currency Comm.*, 91st Cong., 1st Sess. (May 1969).

107. *Id.*

108. It is interesting to note that even Frederick King, president of Hooper-Holmes Bureau has conceded that certain credit keeping is an invasion affected "has initiated a request to the insurance company to gamble thousands of dollars on him." *Prying for Pay: How Credit Bureaus Collect and Use Data*, *The Wall Street Journal*, Feb. 5, 1968, at 16, col. 3.

109. See, e.g., Boeth, *The Assault on Privacy*, *NEWSWEEK*, July 27, 1970, at 16; *A Government Watch On 200 Million Americans?* *U.S. NEWS AND WORLD REPORT*, May 16, 1966, at 56; see also note 6 *supra*.

110. *Hearings on the Computer and Invasion of Privacy Before the Subcomm. of the House Comm. on Government Operations*, 89th Cong., 2d Sess. (1966), at 61.

111. The inter-communication between computerized data banks is commonly referred to as the ability to "interface." 'Interface' means communicate *i.e.*, questions asked at one station can receive answers from another station.

112. The exchanging of information among the agencies was granted Congressional approval in a statute which authorized "A Federal agency to make available to another Federal agency information obtained from any person." 14 U.S.C. § 3507 (1968).

113. As Professor Miller has stated at a symposium conducted on the computer-privacy problem:

Modern information transfer technology in time will prove to be the heart of new communications network, a communications network that differs from many of the communication networks that we are familiar with, such as telephones, telegraph, radio, television and newspapers, only in technological and media terms. Accordingly, the computer must be dealt with as a communication network.

Symposium supra note 7, at 1127.

tween computer networks has certain demonstrated advantages, a substantial danger exists that this new technology will permit serious invasions into an individual's privacy.

Proposed Solutions

A New Federal Agency

The threat to personal privacy through the use of computerized data networks and the lack of existing, clearly defined common law or constitutional safeguards suggest the need for federal legislative remedies.¹¹⁴ Although legal protection may flow from the judicial establishment of information as a property right, or in a misappropriation type tort theory, these doctrines are inappropriate because they were formulated for different purposes, and they do not adequately cover the subject. Congressional action into this area is thus necessary in order to establish and enforce the needed regulations.

Administrative treatment of computerized information may prove to be the most effective means of safeguarding privacy.¹¹⁵ Federal control of this area is the most logical choice due to the distinct national character of present intercommunications between computer networks.¹¹⁶ The establishment of a new federal agency specifically designed to deal with computer systems would be an effective solution for the problems of protecting privacy.¹¹⁷ By means of Congressional legislation, the new agency could be established with authority to fashion a comprehensive set of regulations governing the collection, access, release, and correction of information in computer data banks. With the centralization of regulation, inconsistent interpretations could thus be avoided while providing the needed flexibility which a single legislative bill on privacy cannot accomplish. Furthermore, the adminis-

114. See generally, Westin, *Legal Safeguards to Insure Privacy in a Computer Society*, COMMUNICATIONS OF THE ACM, Vol. 10 (Sept. 1967) at 533.

115. See generally Arpaia, *The Independent Agency—A Necessary Instrument of Democratic Government*, 69 HARV. L. REV. 483 (1955); Friendly, *A Look at the Federal Administrative Agencies*, 60 COLUM. L. REV. 429 (1960); But compare the contention that administrative agencies do not adequately perform their assigned tasks. Hector, *Problems of the CAB and the Independent Regulatory Commission*, 69 YALE L.J. 931 (1960).

116. For a discussion of the regulatory aspects of data transmission between computers see, Note, *Regulations of Computer Communication*, 7 HARV. JOURN. ON LEG., 208 (1970); see also Note, *Computer Services and the Federal Regulation of Communications*, 116 U. PA. L. REV. 328 (1968).

117. The concept of an independent agency has been considered by Senator Ervin and other commentators before Congressional committees. They have maintained that such a new agency acting as an ombudsman or overseer is the only practical method to insure the proper treatment of this field. See Remarks of Senator Ervin, 115 Cong. Rec. (daily ed. Nov. 10, 1969); *Hearings on Federal Data Banks* 831 (Remarks of Alan F. Westin); ASSAULT ON PRIVACY 228-38.

trative approach can provide an easier and less expensive method of resolving disputes between citizens and data banks than can be obtained through litigation which would otherwise be required.¹¹⁸

The most important provisions which should be included in Congressional delegation of authority to the new information agency are the procedural safeguards designed to give notice to the individual of the content of information concerning him, the group requesting such information, and an opportunity to respond. This provision would be consistent with the ideals of fair play and substantive due process and would most likely result in a far greater public acceptance of the information handling process. A review board should also be established whose function would be to expand the agency's rules and methods in order to meet new situations which arise.¹¹⁹ By authorizing a broad range of measures to aid in carrying out the powers conferred in the enabling statute, the review board should shape its policy in the context of rapidly advancing technology without the need for further legislative action in each instance.¹²⁰

Other powers of any agency which might be established that demand serious consideration are: some type of an advisory board, inspectors, ombudsman,¹²¹ or internal-external auditors to review the work of the agency; technical safeguards to assure privacy and security for data during transmission and storage;¹²² and, a licensing or certification system to enforce high standards of those companies handling sensitive information.¹²³

The difficulty in establishing a new agency is the result of understandable congressional hesitancy in adding a separate unit to an already large federal bureaucracy and due to the high cost of funding such a project. These factors, however significant, should not be permitted to be the overriding

118. Cf. M. BERNSTEIN, *REGULATING BUSINESS BY INDEPENDENT COMMISSION* (1955).

119. For an excellent commentary on the role of agency review boards, see Fuchs, *The New Administrative State: Judicial Sanction for Agency Self-Determination in the Regulation of Industry*, 69 COLUM. L. REV. 216 (1969); See also Freedman, *Review Boards in the Administrative Process*, 117 U. PA. L. REV. 546 (1969).

120. Cf. Curtis, *A Better Theory of Legal Interpretation*, 3 VAND. L. REV. 407, 415 (1950); Note, *Intermediate Appellate Review Boards for Administrative Agencies*, 81 HARV. L. REV. 1325 (1968); Fitzgerald, *Trends in Federal Administrative Procedure*, 19 SW. L.J. 239 (1965).

121. See e.g. Davis, *Ombudsmen in America: Officers to Criticize Administrative Action*, 109 U. OF PA. L. REV. 1057 (1961).

122. One writer has viewed the security aspect of computerized files as an issue of a constitutional dimension. See Karst, *supra* note 30, at 343. See also, Ware, *Security and Privacy in Computer Systems*, PROCEEDINGS, 1967 SPRING JOINT COMPUTER CONFERENCE, 279-90 (1967); Fanwick, *Computer Safeguards: How Safe are They?*, SDC MAGAZINE July-Aug., 1967 at 26, 27; Bigelow, *Legal and Security Issues Posed by Computer Utilities*, HARV. BUS. REV. Sept.-Oct. 1967, at 15.

123. Personnel could also be licensed, bonded and insured.

consideration for rejection of this proposal if privacy is to continue to be a valued right in America.

F.C.C. Regulation

The legislative expansion of regulatory authority within an existing agency is a possible alternative to the development of a new agency. The selection would naturally emanate from those agencies dealing with computer communication and information industries.¹²⁴ Although certain agencies are worthy of consideration, *e.g.*, as the Federal Trade Commission, the Census Bureau and the Office of Management, the Federal Communications Commission (F.C.C.) is in the best position to most adequately handle this area.¹²⁵

The F.C.C. derives its authority under the Communication Act of 1934¹²⁶ which gives it responsibility to regulate "all interstate and foreign communication by wire and radio."¹²⁷ The Act does not create a general right of privacy, but Sec. 605 which forbids unauthorized interception between communication links, bears directly on this matter. Primarily due to the inadequate record of Congressional objectives in passing Sec. 605, its scope and application has never been sufficiently defined.¹²⁸

From 1966 to 1968, the F.C.C. conducted a comprehensive inquiry¹²⁹ into computer communication and privacy implications.¹³⁰ As a result of the

124. In 1968, President Johnson included in a special Task Force a study of the regulatory policy of data communication. FINAL REPORT, PRESIDENT'S TASK FORCE ON COMMUNICATIONS POLICY (1968).

125. "The further the carriers move into data processing, however, and the more suggestive their services because of a computer utility, the more likely it is that the F.C.C. will begin to regulate at least certain segments of the data processing market." Irwin, *The Computer Utility: Competition or Regulation?*, 76 YALE L.J. 1299, 1311 (1966).

126. 47 U.S.C. §§ 151-609 (1964).

127. 47 USC § 605.

128. "Privacy particularly in the area of communications, is a well established policy and objective of the Communications Act. Thus, any threatened or potential invasion of privacy is cause for concern by the Commission and the industry. In the past, the invasion of information privacy was rendered difficult by the scattered and random nature of individual data. Now the fragmentary nature of information is becoming a relic of the past. Data centers and common memory drums housing competitive sales, inventory and credit information and untold amount of personal information must remain free from unauthorized invasion of disclosure, whether at the computer, the terminal station, or the interconnecting communication link." *In the Matter of Regulatory and Policy Problems Presented by the Independence of Computer and Communications Services and Facilities*, FCC Notice of Inquiry, Docket No. 16979, 7 F.C.C.2d 11, 8 P & F Radio Reg. 2d 1567 (Nov. 9, 1966) [hereinafter cited as Computer Inquiry].

129. *Id.*

130. The issues focused upon by the FCC were:

large number of responses from the computer and communication industries,¹³¹ the F.C.C. financed the Stanford Research Institute to evaluate these responses and offer recommendations on possible action.¹³² With the convergence and growing interdependence of computers and communications¹³³ and the compelling need for clarification which might accommodate these changing technologies, the F.C.C. is in a unique position to bring all data communication within its regulatory powers.¹³⁴ Because of its extensive expertise in the communication field, the computer-privacy arena is a natural extension of the F.C.C. regulatory powers. Moreover, none of the F.C.C. Commissioners have expressly refuted this proposition.¹³⁵

The F.C.C. regulations of computer communications could be accomplished by a broad interpretation under the existing purview of the Communications Act¹³⁶ or, if necessary, by a minor legislative expansion of its statutory jurisdiction. Arguments against the F.C.C. regulation generally proceed from such premises as the lack of jurisdiction, a desire to avoid regulation of "program or communication content,"¹³⁷ inadequate staffing, lack of technical expertise, insufficient funding, and an already existing work overload.¹³⁸ However, these complaints are not persuasive because

1. What is the regulatory status of computer-communications services?

2. Are common carrier communications service and tariffs responsive to the requirements of the data processing industry?

3. Can privacy be protected against the increasing phenomenon of concentration and the exchange of data information? S. MATHISON AND P. WALKER, *COMPUTERS AND TELECOMMUNICATIONS: ISSUES IN PUBLIC POLICY*, v. (1970).

131. The Commission received over 60 responses.

132. STANFORD INSTITUTE REPORT NO. 739 B-1-7 (1969).

133. See generally, Irvin, *The Computer Utility: Competition or Regulation?* 76 YALE L. J. 1299 (1966); D. PARKHILL, *THE CHALLENGE OF COMPUTER UTILITY* (1966); P. BARAN, *THE COMING COMPUTER UTILITY—LAISSEZ-FAIRE, LICENSING OR REGULATION?* (1967); C. BARNEET, *THE FUTURE OF COMPUTER UTILITY* (1967).

134. "The traditional lines separating data processing and communications have been softened by the emergence of a new industry, which, for lack of precise description, is known as the data, computer or information utility." Note, *Computer Services and the Federal Regulation of Communications*, 116 U. PA. L. REV. 328 (1967).

135. Interview with Charlotte T. Reid, July 26, 1972; Interview with Richard E. Wiley, July 25, 1972; Interview with Nicholas Johnson, July 11, 1972; Interview with H. Rex Lee, July 20, 1972; Interview with Robert E. Lee, July 7, 1972; Interview with Benjamin L. Hooks, July 14, 1972; Interview with former Commissioner Kenneth Cox, August 2, 1972; Dean Burch was not interviewed.

136. Justice Harlan, expressing the views of the Court, in *United States v. Southwestern Cable Co.*, 392 U.S. 157, 172 (1968), has construed the Communications Act of 1934 in a very liberal fashion. He states: "Nothing in the language of § 152(a), in the surrounding language, or in the Act's history or purposes limits the Commission's authority to those activities and forms of communication that are specifically described by the Act's other provisions. The section itself states merely that the 'provisions of [the Act] shall apply to all interstate and foreign communication by wire or radio. . . .'"

137. ASSAULT ON PRIVACY 232.

138. See note 135, *supra*.

they are not peculiar solely to the F.C.C. and the actual problems presented could be overcome by Congress authorizing the expansion of F.C.C. jurisdiction and the proper funding. Given legislative guidelines to establish policies and standards for the protection of privacy and an increase in its technically trained staff, the F.C.C. could adequately handle the task.

Statutory Remedies

The development of legislation to explicate who is to have access to what information may be achieved by Congressional enactment of a privacy bill.¹³⁹ Federal statutory protection would necessarily entail a comprehensive prescription of policy requirements and a high standard of due care. Prophylactic restrictions against data manipulation, civil sanctions providing a remedy for misbehavior, and an individual's right to withhold certain kinds of information could be included. Provisions requiring confidentiality of information handling and restrictions on the circulation of information would be needed in the legislation. Extensive hearings could also be conducted to provide a forum for interested groups and to insure comprehensive legislation. In addition, a special joint Congressional committee could be established to review all proposed programs.

The Fair Credit Reporting Act of 1970¹⁴⁰ represents a starting point from which legislators might begin to proceed with the task of statutory enactment.¹⁴¹ The Act was designed to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy. Significant provisions under this credit report statute include the following: a requirement that anyone who wishes to use an investigative report¹⁴² disclose to the subject that such a report has been requested and that the subject is entitled to know the nature and scope of the investigation;¹⁴³ a limitation on the purposes for which consumer reports may be given out and that additional uses require either a court order or written permission by the subject;¹⁴⁴ a right of the subject to dispute and make corrections concerning the accuracy of the file;¹⁴⁵ and a statute of limitations for which obsolete data will not be reported.¹⁴⁶

139. For a discussion of a right to privacy act, see Pipe, *Privacy: Establishing Restrictions on Government Inquiry*, 18 AM. U.L. REV. 516 (1969).

140. Pub. L. 91-508 §§ 601-22 (Oct. 26, 1970) 15 U.S.C. § 1878. For a review of this Act, see Note, *An Analysis of the Fair Credit Reporting Act*, 23 BAYLOR L. REV. 616 (1971).

141. § 602(a)(4); See generally SHARP, CREDIT REPORTING AND PRIVACY (1970).

142. Fair Credit Reporting Act § 603(e).

143. *Id.* § 606.

144. *Id.* § 604.

145. *Id.* § 611.

146. *Id.* § 605.

The prospect, however, of extensive legislation in such an extremely complicated area is not promising. This outlook is the product of the very narrow scope of current proposals,¹⁴⁷ Congressional deficiency in technical expertise, natural inertia, the difficulty in categorizing levels of sensitive or privileged information, and a fear of enacting obsolete legislation due to the rapidly changing computer and communication industries.¹⁴⁸ Hence, a comprehensive legislative solution is not likely despite more satisfactory attempts in other countries.¹⁴⁹

The construction of an entirely new and separate data network to handle the increasing data traffic has been proposed.¹⁵⁰ Although only briefly explored in its *Computer Inquiry*, the F.C.C. conceded that the present telephone network was not built for data transmission and it therefore had many characteristics which would have to be changed.¹⁵¹ Since it has been predicted that by 1980 as much as half of the usage of the telephone network may be the result of data rather than telephone traffic,¹⁵² this suggestion demands serious consideration. An advisory board similar to that recommended under the F.C.C. regulation could be added which would provide the prerequisite supervision. Nonetheless, the enormous problem of dealing with the many competing interests in establishing a new separate data network and the slight past attention given to this proposal, indicate that the proposal is not feasible at this juncture.

Self Regulation

Self-regulation by the computer industry has also been suggested and analyzed to the present successful self-regulating National Association of Security Dealers.¹⁵³ According to this proposal, the communication industry would cooperate with the computer industry "to adopt and implement, under the auspices of the federal government, a comprehensive system of self-regulation to ensure the privacy and security of data."¹⁵⁴ But a proposal of this nature does not seem to be entirely realistic in view of the distinct limited recognition given to privacy by the industry respondents in the *Computer Inquiry*. The respondents showed greater attention to the cost increase when

147. See note 2, *supra*.

148. Interview Senator Ervin, in Washington D.C., April 16, 1972.

149. ASSAULT ON PRIVACY 227.

150. U.S. National Commission on Technology, Automation and Economic Progress, *Technology and the American Economy*, 252 (1966).

151. COMPUTER INQUIRY 24.

152. *Id.*

153. For a discussion which proposes self-regulation by the computer industry under federal government auspices, see Grenier, *Computers and Privacy: A Proposal for Self-Regulation*, 1970 DUKE L. J. 495, 505 (1970).

154. *Id.*, at 496-97.

protecting privacy than to a serious encounter with the importance of personal privacy. The inclusion of a sophisticated code of ethics into the highly vague functional aspects of self-regulation and its enforcement probably will not change the situation.

Other Proposals

A "bill of rights"¹⁵⁵ for computerized information and a "data bank on data banks"¹⁵⁶ are additional minor proposals. The bill of rights might help extinguish the barrier between the individual and information concerning him and the "data bank on data banks" could perform the functions of a private monitoring system.¹⁵⁷ Despite these apparent advantages, both proposals are severely incomplete and not easily workable and should be evaluated only in the context of a larger regulatory scheme discussed above.¹⁵⁸

Conclusion

It is time for Congress to establish a new federal agency to control the collection, storage, dissemination, and usage of information in computer data banks. The urgency of this appeal is emphasized by the present lack of effective legal protection and the greatly increasing intercommunication between data banks.¹⁵⁹ While it is conceded that minimal encroachments upon privacy are the inevitable price for order and progress in modern living, irresponsible and unreasonable invasions should not be tolerated even

155. McCarthy, *Information*, 215 SCIENTIFIC AMERICAN 3 (Sept. 1966).

156. *Hearing on Federal Data Banks*, 634 [Remarks of Alan F. Westin].

157. *Id.*

158. For example, on May 23, 1968, Senator Edward Long proposed an amendment which would give recognition to a right of privacy. The amendment said:

The Constitution of the U.S. guarantees to all individuals a basic right of privacy. Accordingly, the Congress endorses the requirement that what an individual seeks to preserve as private is to be protected, even in an area accessible to the public. The Congress supports the view that wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures.

On a voice vote, however, the proposed amendment was defeated. Cong. Rec. S 6202. Amendment 717.

159. Three major studies have been conducted on the subject of the computer network systems: *Report of the Comm. on the Preservation and Use of Economic Data to the Social Science Research Council*, in *Hearings on the Computer and the Invasion of Privacy Before a Subcomm. of the House Comm. on Government Operations*, 89th Cong., 2d Sess. 195 (1966); *Statistical Evaluation Report No. 6—Review of Proposal for a National Data Center*, in *Hearings on the Computer and Invasions of Privacy Before a Subcomm. of the House Comm. on Government Operations*, 89th Cong., 2d Sess. 254 (1966); *Report of the Task Force on the Storage of and Access to Government Statistics*, in *Hearings on Computer Privacy Before a Subcomm. on Administrative Practice and Procedure of the Senate Comm. on the Judiciary*, 90th Cong., 1st Sess. 25 (1967).

though such occurrences are rapidly becoming a way of life.¹⁶⁰

In order to provide immediate attention to the information-privacy area an independent study and planning Commission should be established. The purpose of the Commission would be to study and recommend appropriate affirmative action since the congressional hearings to date have merely restated prior complaints. The proposed commission would consist of representatives from Congress, federal agencies, the communication and information industries, and other experts in the field. Special hearings designed to place special emphasis upon individual needs should then be held to ensure that the most beneficial resolution is achieved. The Commission should begin with an analysis of the conclusions reached by two major investigations which are currently taking place.¹⁶¹ In addition, the Commission should make an arrangement whereby it will meet periodically in order to provide further studies as needed.

In light of contemporary needs, the work of Congress has been largely deficient in the computer data bank-privacy arena. Most importantly, an independent commission would assure that proper attention is immediately focused upon this field while providing an extensive examination of the problems involved. Irrespective of the commission's final solution, the deep respect for the importance of the individual and his "right to be let alone" must not succumb to the demands of efficiency. Once the right of privacy is allowed to carelessly erode, it will be difficult to restore. There are unmistakable signs that the process of erosion has already begun.

Grant Morris

160. For example, in 1970 a former Army officer disclosed that the Army, since 1965, had been collecting information on civilians at Fort Holabird in its computer data bank. The purpose of this operation was to enable the Army to anticipate civil disturbances. Pyle, *CONUS Intelligence: The Army Watches Civilian Politics*, WASH. MONTHLY, Jan. 1970, at 4. Immediately afterward, however, Secretary Laird announced that the operation was to be terminated. Beecher, *Laird Acts to Tighten Rule over Military Intelligence*, N.Y. Times, Dec. 24, 1970, at 1, col. 2.

161. The two investigations are: the National Academy of Sciences which is headed by Alan Westin of the Columbia University and the National Science Foundation which is headed by Arthur R. Miller of the University of Michigan.